

## 基于双混沌系统互反馈的加密算法

毛永毅, 王 瑶\*

(西安邮电大学 电子工程学院, 西安 710061)

(\*通信作者电子邮箱 wangyaoping99@163.com)

**摘 要:**为使低维混沌加密系统具有较高的安全性和良好的运算效率,提出一种基于 Logistic 映射和 Tent 映射的复合混沌加密系统。通过两种映射互反馈产生密钥序列,再对读取的明文进行加密;同时利用密文反馈的方式来改变混沌映射的迭代次数,使迭代过程具有一定的随机性。结果表明,与单一的 Logistic 混沌加密相比,该算法具有很大的密钥空间、较高的加密强度和低维混沌加密系统的良好运算效率,而且能有效地抵抗穷举攻击、统计学攻击和相图攻击。

**关键词:**混沌; Logistic 映射; Tent 映射; 混沌加密; 互反馈

**中图分类号:** TP309.2 **文献标志码:** A

### Encryption algorithm based on double chaos system with mutual feedback

MAO Yong-yi, WANG Yao\*

(School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an Shaanxi 710061, China)

**Abstract:** In order to increase the security of the low dimensional chaotic encryption system while not affecting the performance, a composite chaotic encryption system based on Logistic mapping and Tent mapping was presented. Firstly, the secret-key sequences were generated based on two mapping with mutual feedback, which was used to encrypt the plaintext; at the same time, the number of chaotic iterations was changed through cipher-feedback, and the iterative process has certain randomness. The results show, compared with single Logistic chaotic encryption, the algorithm not only has a large key space, high encryption intension and good operation efficiency of low dimensional chaotic encryption system, but also can resist brute-force attack, statistical attack and phase diagrams attack effectively.

**Key words:** chaos; Logistic mapping; Tent mapping; chaotic encryption; mutual feedback

## 0 引言

随着信息化的不断发展及因特网的迅速普及,信息安全问题已显得尤为重要。这样就必然要对信息进行安全的加密防护措施。近年来,将混沌理论应用于信息加密是当今国内外学者研究加密技术的一个热点<sup>[1-2]</sup>。混沌是一种无规则的运动,是在非线性系统中出现的确定性的、抽象的类随机过程(类随机性),它具有对初始值和系统参数的极度敏感性、有界性、轨道不可预知性<sup>[3]</sup>、遍历性等优良特性,使得它非常适用于保密通信和数据安全等众多领域。

当前利用混沌设计信息加密算法有多种,文献[4-6]中的混沌加密算法都采用单混沌系统,虽具有良好的加密速度,但其密钥空间很小,且算法相对简单,安全性不高;文献[7-10]是将单一算法进行改进,在安全性方面得到提高,能有效抵抗差分攻击、统计攻击等一般的攻击,但在加密速度和抗干扰性方面较差且周期较短;文献[11-14]中的算法增大了密钥空间且具有较高的安全性,但因其构造复杂、计算精度要求较高且周期长而不利于实际应用。针对以上研究现状,考虑有效利用低维混沌加密的良好运算速度和高维混沌加密的大密钥空间的优点,选取合理的混沌加密算法以增强加密算法的安全性。

本文提出基于一维 Logistic 映射和 Tent 映射的复合混沌映射,在特定初始值和参数下进行迭代,并且相互反馈后产生

混沌子密钥序列对明文进行加密。此方法一方面有效地增加了密钥空间,增强了算法抗穷举攻击的能力;另一方面在利用反馈产生子密钥时,子密钥除了与初始值和参数相关外,还在一定程度上与明文和密文有关,这样就能有效地防止对已知明文和选择明文分析,以免信息泄露。

## 1 Logistic 映射和 Tent 映射

### 1.1 Logistic 映射

Logistic 映射是一种最典型的,并且非常简单的却被广泛应用的一维映射,它的动力学方程为:

$$x_{n+1} = \mu * x_n * (1 - x_n) \quad (1)$$

其中:  $\mu \in [0, 4]$ ,  $x_n \in (0, 1)$ ,  $n = 1, 2, \dots$ 。

Logistic 映射是一个简单的非线性方程,但这个映射体现着现代混沌理论的最基本思想,它包括倍周期到混沌区、分岔图等非线性理论的模式和基本框架, $\mu$  为其分支参数。由文献[15]中的分岔图可知,当  $1 \leq \mu < 3.0$  时,系统的稳态解为不动点,即周期 1 解;当  $\mu = 3.0$  时,系统稳态解由周期 1 变为周期 2,称为二分叉过程;当  $\mu = 3.449489$  时,系统稳态解由周期 2 变为周期 4;当  $\mu = 3.544090$  时,系统稳态解由周期 4 分为周期 8;当  $\mu = 3.5699456$  时,系统稳态解为周期  $2^\infty$  解;因此,当  $3.5699456 \leq \mu \leq 4$  时,Logistic 映射进入混沌状态。

当 Logistic 映射进入混沌状态后,此时控制参数  $\mu$  的取值为  $3.5699456 \leq \mu \leq 4$ ,但当  $\mu$  取某些值时在混沌区出现一些

收稿日期: 2012-04-05; 修回日期: 2012-05-17。

基金项目: 陕西省自然科学基金资助项目(2009JM 8015); 陕西省教育厅专项(2010JK815)。

作者简介: 毛永毅(1969-),男,湖南长沙人,教授,博士,主要研究方向: 通信与信息处理、移动台定位; 王瑶(1987-),男,陕西宝鸡人,硕士研究生,主要研究方向: 数字信号处理与系统实现。



当 ASCII 码值大于 127 的字符均为不可显示的字符)。

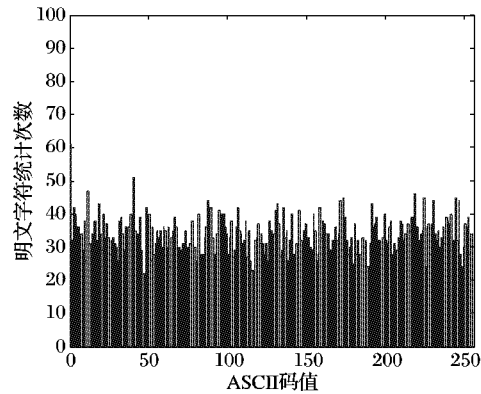


图5 错误解密后的明文统计直方图

对比文献[9]中由单一的Logistic映射通过 $M$ 次迭代后,

表1 算法的密钥空间对比

算法	密钥组成	含义	取值范围	空间大小	总的密钥空间大小
文献[9]算法	$\mu$	参数	$3.569\,945\,6 \leq \mu \leq 4$	$0.43 \times 10^{16}$	$0.43 \times 10^{32}$
	$x_0$	初始值	$(0,1)$	$1 \times 10^{16}$	
本文算法	$\mu, \lambda$	参数	$3.569\,945\,6 \leq \mu \leq 4, 1.4 \leq \lambda \leq 2$	$0.258 \times 10^{32}$	$0.258 \times 10^{48}$
	$x_0$	初始值	$(0,1)$	$1 \times 10^{16}$	

表2 算法的密文统计方差和解密时间

算法	密文统计方差	时间/s	
		加密	解密
文献[9]的算法	61.926 1	0.657	0.672
本文算法	32.900 8	0.703	0.735

3.2 算法的安全性分析

1) 初值的敏感性分析。文献[15]中分析了Logistic映射处于混沌状态时初始值变化0.000 000 1,控制参数和迭代次数均不变时,经Logistic迭代大概18次时,两个序列已产生很大的差异;同样本算法中取 $x_1 = 0.623\,45, x'_1 = 0.623\,450\,1$ ,其他与文献[15]条件相同,在迭代16次时序列产生极大差异,因此可以看出本算法对初始值也极其敏感,且敏感性比文献算法较好,如表3所示为文献算法与本文算法随迭代次数变化的序列差的对比。

表3 文献算法和本文算法随迭代次数变化的序列值差异对比

迭代次数 $n$	文献[15]算法 (序列差 $ X_1 - X_2 $ )	本文算法 (序列差 $ X_1 - X_2 $ )
1	0.000 1	0.000 1
2 ~ 11	0.000 0	0.000 0
12	0.000 0	0.000 1
13	0.000 1	0.000 1
14	0.000 2	0.000 2
15	0.000 1	0.000 1
16	0.000 2	0.000 6
17	0.000 1	0.001 2
18	0.002 2	0.002 3
19	0.001 7	0.003 9
20	0.002 8	0.007 1

注:此处设两个序列值差允许最大为0.000 2时,可视两个序列值相同;且列出了迭代20次的差值。

经分析,此系统的控制参数最大误差可达到 $10^{-14}$ 时,便不能正确解密;其次,上述已经表明本算法具有较大的密钥空间。这足以说明本文所设计的系统具备抗穷举攻击的能力。

2) 统计学分析。由仿真图可以看出,未加密的明文字符

将得到的值取小数点后 $N$ 位,再取模256后得出密钥,再对明文加密,其初始密钥只取Logistic映射的初始值 $x_1$ ,控制参数 $\mu$ 、初始迭代次数 $M$ ,本文所设计的算法初始取5个参数作为密钥,分别为Logistic映射的初始值 $x_1$ 、控制参数 $\mu$ 、初始迭代次数 $b$ ,Tent映射的控制参数 $\lambda$ 、初始迭代次数 $b'$ 。表1为不同算法的密钥空间对比。

由表1可看出本文算法比文献[9]算法的密钥空间大将近 $10^{16}$ 倍,所以,该算法只在考虑具有良好运算效率的基础上,与同类算法相比一定程度地增大了密钥空间,系统的安全性较高,但要达到高维混沌加密系统的密钥空间 and 安全性,还需要进一步研究。

对比文献[9],由表2仿真数据看出,文献[9]的密文统计方差几乎是本文算法的2倍,且两种算法加、解密时间相差不大,故该算法在保持低维良好运算速度优点的同时具有比单一加密算法更高的加密强度。

(图3)出现的次数最大可达350,本文加密算法充分利用了较大的密钥空间,使得相对比较集中的明文字符经过本文所设计的系统加密后密文字符能比较均匀地分布,加密后的密文字符出现次数最多不到50次(图4),这说明加密后的密文信息已经完全掩盖了明文信息,其统计特性有很大的变化;文献[9]中的算法同样可达到加密效果,但同一篇明文加密后的密文一些字符出现次数已经达到60。显然本文加密系统具有很好的抗统计学攻击能力。

3) 抗相图攻击。文献[4-5]中未经设计的Logistic映射和Tent映射的混沌加密系统相图如图6(a)、(b)所示,本文的复合混沌加密系统相图如图6(c)所示。

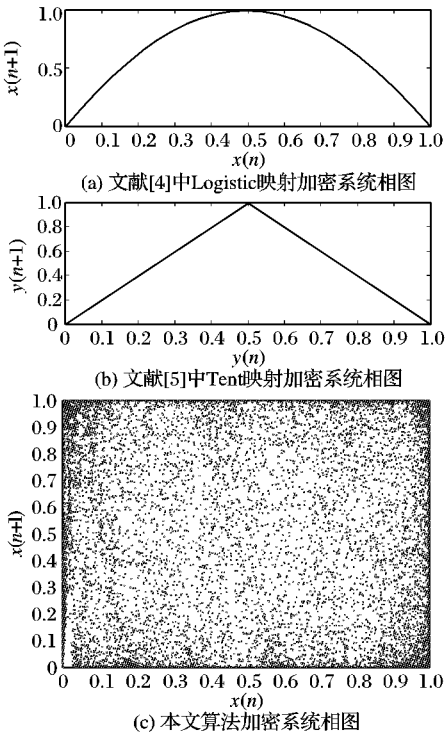


图6 混沌加密系统相图比较



- king Conference. Piscataway, NJ: IEEE Press, 2009: 1128 - 1132.
- [4] 张志勇, 牛丹梅. 数字版权管理中数字权利使用控制研究进展[J]. 计算机科学, 2011, 38(4): 48 - 54.
- [5] 林丽, 李艳, 关德军. 数字版权管理系统中安全模型的研究与设计[J]. 通化师范学院学报, 2011, 32(10): 14 - 16.
- [6] 张晓林. 数字权益管理技术[J]. 现代图书情报技术, 2001(5): 3 - 10.
- [7] ZENG WENJUN, LEI S. Efficient frequency domain selective scrambling of digital video[J]. IEEE Transactions on Multimedia, 2003, 5(1): 118 - 129.
- [8] 曾婷, 张成昱, 肖燕. 电子图书数字权限管理系统比较研究[J]. 图书馆杂志, 2004, 23(8): 55 - 60.
- [9] 徐新光. 数字版权管理的技术和难题[J]. 广播与电视技术, 2006, 33(12): 75 - 79.
- [10] CHOR B, FIAT A, NAOR M. Tracing traitors[C]// CRYPTO'94: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1994: 257 - 270.
- [11] CHOI S, HAN J, JUN S I. Improvement on TCG attestation and its implication for DRM[C]// ICCSA'07: Proceedings of the 2007 International Conference on Computational Science and Its Applications. Berlin: Springer-Verlag, 2007: 912 - 925.
- [12] ABBADI I M, ALAWNEH M. Replay attack of dynamic rights within an authorised domain[C]// SECURWARE'09: Proceedings of the 2009 the Third International Conference on Emerging Security Information, Systems and Technologies. Washington, DC: IEEE Computer Society, 2009: 148 - 154.
- [13] BHATT S, SION R, CARBUNAR B. A personal mobile DRM manager for smartphones[J]. Computers and Security, 2009, 28(6): 327 - 340.
- [14] 张海鑫, 程丽红, 李顺东. 数字版权管理系统中的使用控制模型[J]. 计算机技术与发展, 2009, 19(12): 135 - 157.
- [15] PARK J, SANDHU R. The UCON<sub>ABC</sub> usage control model[J]. ACM Transactions on Information and System Security, 2004, 7(1): 128 - 147.
- [16] PARK J, SANDHU R. Towards usage control models: Beyond traditional access control[C]// Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2002: 57 - 64.
- [17] ZHANG X W, PARISI-PRESICCE F, SANDHU R, *et al.* Formal model and policy specification of usage control [J]. ACM Transactions on Information and System Security, 2005, 8(4): 351 - 387.
- [18] KATT B, ZHANG X W, BREU R. A general obligation model and continuity-enhanced policy enforcement engine for usage control [C]// Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2008: 123 - 132.
- [19] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612 - 613.
- [20] BLACKLEY G R. Safeguarding cryptographic keys[C]// Proceedings of the National Computer Conference. Washington, DC: IEEE Computer Society, 1979: 313 - 317.

(上接第2770页)

因为单一的混沌序列都是由确定性的方程产生,理论上攻击者可以通过相空间重构的方法对加密信息进行破译。

从图6的相图分析可得出,单一的未经设计的加密混沌系统是单一的曲线,很容易受到攻击;而本文设计的加密系统相图是无规律的,这无疑对采用相图进行攻击的攻击者来说,是很难实现的。

#### 4 结语

基于单一混沌加密算法实现简单,但密钥空间小,安全性差。本文设计了一种基于双混沌互反馈的数据加密算法,采用 Logistic 映射和 Tent 映射两个单一混沌映射利用给定初始值  $x_1$  和控制参数  $\mu, \lambda$ , 初始迭代次数  $b, b'$  再进行迭代后将值进行互反馈得出子密钥序列,使密文具有不可预测性。通过以上对该算法的仿真分析可知,此算法取得了很好的加密和解密效果;再通过改变参数进行加解密可得此混沌系统对初始条件极其敏感。最后进一步对设计的混沌加密系统进行安全性分析可知此算法密钥空间大且加密强度高,能有效防止攻击者利用穷举、统计、相图进行的攻击,是比较安全可靠的,而且具有很好的应用前景。

#### 参考文献:

- [1] 包浩明, 朱义胜. 基于多层密钥的混沌映射保密通信系统[J]. 电子学报, 2009, 37(6): 1222 - 1225.
- [2] 李永华, 王冰. 基于混沌序列的图像加密算法[J]. 计算机应用, 2009, 29(5): 100 - 102.
- [3] 晋建秀, 丘水生. 基于物理混沌的混合图像加密系统研究[J]. 物理学报, 2010, 59(2): 792 - 799.
- [4] 谢建全, 阳春华, 黄大足, 等. 基于 Logistic 映射的加密算法的安全性分析与改进[J]. 小型微型计算机系统, 2010, 31(6): 1073 - 1076.
- [5] 叶瑞松, 庄乐仪. 基于帐篷映射迭代的置乱方法[J]. 计算机应用, 2009, 29(10): 2713 - 2715.
- [6] 郭建胜, 张锋. 一种图像加密算法的等效密钥攻击方案[J]. 电子学报, 2010, 38(4): 781 - 785.
- [7] XIE JIANQUAN, YANG CHUNHUA, XIE QING, *et al.* An encryption algorithm based on transformed Logistic map[C] // International Conference on Networks Security, Wireless Communications and Trusted Computing. Washington, DC: IEEE Computer Society, 2009: 111 - 114.
- [8] 徐淑英, 王继志. 一种改进的混沌迭代加密算法[J]. 物理学报, 2008, 57(1): 37 - 41.
- [9] 赵雪章, 席运江. 一种基于混沌理论的数据加密算法设计[J]. 计算机仿真, 2011, 28(2): 120 - 123.
- [10] GUO WEN-PING, CHEN YING. Chinese character encryption algorithm based on Logistic mapping[C]// 2010 3rd IEEE International Conference on Computer Science and Information Technology. Washington, DC: IEEE Computer Society, 2010: 478 - 481.
- [11] 王静, 蒋国平. 基于密文反馈的 Logistic 映射认证加密算法[J]. 东南大学学报, 2010, 40(9): 84 - 91.
- [12] 李恩, 吴敏, 熊永华. 一种基于双混沌映射的加密算法设计与应用[J]. 计算机应用研究, 2009, 26(4): 1512 - 1514.
- [13] 董斌辉, 周健勇. 混沌随机全排列置换加密算法及应用[J]. 计算机工程与应用, 2011, 47(8): 59 - 61.
- [14] 张永, 温涛, 郭权, 等. 混沌同步密钥流生产算法评价方法[J]. 计算机工程与应用, 2010, 46(20): 68 - 70.
- [15] 刘成斌. 混沌加密算法的研究与实现[D]. 北京: 北京邮电大学, 2008.